CLAIMS

1. (Currently Amended) In a host of a virtual machine environment having one or more methods in a shared managed library, a process for managing calls from a first managed code caller to a first method, the process managing calls based on a hosting rule selected from the following hosting rules each stored in a data structure:

authorizing, by a computing device, calls from one of a plurality of managed code callers to the first method;

preventing, by the computing device, calls from one of a plurality of managed code callers to the first method due to the first method's inappropriateness for the virtual machine environment, the first method's inappropriateness being indicated by a query that determines whether a host protection custom attribute (HPCA) is associated with the first method, the query determining from the HPCA that the calls from one of the plurality of managed code callers are to be prevented when the HPCA is associated with the first method; and

conditionally authorizing, by the computing device, calls from one of a plurality of managed code callers to the first method based on the first method's required level of trust, [[and]] a level of trust attributed to the first managed code caller, and a rule demand that contains data quantifying a degree of the level of trust, the level of trust attributed to the first managed code caller corresponding to an identity of a provider of the first managed code caller.

2. (Canceled)

3. (Previously Presented) The process as defined in Claim 1, wherein the authorizing and the preventing a call further comprises:

compiling code corresponding to the first managed code caller into native code; and

executing the native code corresponding to the first managed code caller while the first managed code caller is making the call to the first method native code.

4. (Previously Presented) The process as defined in Claim 3, further comprising throwing an exception during the executing and while the first managed code caller is making the call to the first method native code when:

the call is prevented; or

the level of trust attributed to the first managed code caller is insufficient when compared to a security permission demand assigned to and required by the first method.

5. (Previously Presented) The process as defined in Claim 1, wherein when the call from the first managed code caller is authorized, access is provided by the first method to a protected resource.

6. (Previously Presented) The process as defined in Claim 1, wherein any authorized call provides one or more of the plurality of managed code callers with access to one or more protected resources corresponding to the called method.

7. (Canceled)

8. (Previously Presented) The process as defined in Claim 1, wherein the host compiles the first managed code caller into native code that is executed by a common language runtime via an operating system of the host.

9. (Previously Presented) The process as defined in Claim 1, further comprising configuring each method in the shared managed library with one hosting rule.

10. (Previously Presented) The process as defined in Claim 9, wherein each method is configured prior to any call to any method from any one of the plurality of managed code callers.

11. (Previously Presented) The process as defined in Claim 1, further comprising:

determining whether the host will use any hosting rule in authorizing a call from any one of the plurality of managed code callers to any of the one or more methods; and

configuring the one or more methods in the shared managed library with one hosting rule when the determination is affirmative, and not configuring the one or more methods in the shared managed library with one hosting rule when the determination is negative.

12. (Previously Presented) The process as defined in Claim 11, wherein:

each method in the shared managed library provides access to one or more protected resources; and

the host has access to a host configuration data structure comprising:

resource checking data for making the determination;

configuration data referencing the one or more protected resources and specifying:

each protected resource to which access will be authorized to any one of the plurality of managed code callers;

each protected resource to which access will be prevented to any one of the of managed code callers; and

each protected resource to which access will be authorized to any one of the plurality of managed code callers having a recognized level of trust satisfying a security permission demand corresponding to the protected resource;

wherein the process further comprises:

accessing the host configuration data structure; and

using the resource checking data in the host configuration data structure to make the determination, wherein the configuring of the one or more methods in the shared managed library with one hosting rule comprises, for each method:

matching each protected resource to which the method provides access to the corresponding protected resource in the host configuration data structure; and

for each match, assigning to the method the corresponding configuration data that is associated with the protected resource in the host configuration data structure.

13. (Previously Presented) A computer readable storage medium having machine readable instructions stored thereon that, when executed by one or more processors, causes the one or more processors to implement the process as defined in claim 1.

14. (Currently Amended) A method, comprising:

intercepting, with a computing device having a host operating in a managed environment, a call from a managed caller to a managed callee; and

deriving, by the computing device, whether the call is permissible according to the host's prior configuration of a plurality of managed callees, wherein:

each managed callee provides access to a protected resource; and

the prior configuration specifies whether to:

authorize the call to be made;

prevent the call to be made, the preventing being indicated by a query that determines whether a host protection custom attribute (HPCA) is associated with a method, the query determining from the HPCA that the calls from the managed code caller is to be prevented when the HPCA is associated with the method; or

conditionally authorize the call to be made based upon the degree to which the host trusts the managed caller, the degree to which the host trusts the managed caller corresponding to an identity of a provider of the managed caller and a rule demand that contains data quantifying the degree to which the host trusts the managed caller,

providing access, by the computing device, to the protected resource to the managed caller when the call is permissible; and

preventing access, by the computing device, to the protected resource to the managed caller when the call is not permissible.

15. (Canceled)

16. (Canceled)

17. (Previously Presented) The method as defined in Claim 14, wherein the host compiles the managed caller into native code that is executed by a common language runtime via an operating system of the host.

18. (Previously Presented) The method as defined in Claim 17, further comprising throwing an exception when:

the managed caller attempts to make a call that is prevented; or

the managed caller attempts to make a call when the degree to which the host trusts the managed caller is insufficient.

19. (Previously Presented) The method as defined in Claim 14, further comprising, prior to the intercepting:

determining whether the host will perform the deriving;

performing the intercepting and the deriving if the determination is affirmative; and

preventing the intercepting and the deriving if the determination is negative.

20. (Previously Presented) The method as defined in Claim 19, wherein:

the host has access to a host configuration data structure comprising:

resource checking data for making the determination; and

configuration data sufficient for the host's prior configuration of the plurality of managed callees;

the determining whether the host will make the derivation comprises accessing, with the host, the resource checking data in the host configuration data structure.

21. (Previously Presented) A computer readable storage medium having machine readable instructions stored thereon that, when executed by one or more processors, causes the one or more processors to implement the method as defined in claim 14.

22. (Currently Amended) An apparatus, comprising:

virtual machine means, in a managed code portion including a plurality of methods in a shared managed library, for operating a plurality of managed code callers in the managed code portion;

execution engine means, in a native code portion, for the virtual machine means;

means, in a native code portion, for providing a runtime engine in an operating system; and

means for authorizing or preventing a call from a first one of the plurality of managed code callers to a first one of the plurality of methods based upon a configuration of the first method with a hosting rule selected from a group comprising of:

authorizing calls from any one of the plurality of managed code callers to the first method;

preventing calls from any one of the plurality of managed code callers to the first method due to the first method's inappropriateness for the runtime environment, the first method's inappropriateness being indicated by a query that determines whether a host protection custom attribute (HPCA) is associated with the first method, the query determining from the HPCA that the calls from any one of the plurality of managed code callers are to be prevented when the HPCA is associated with the first method; and

conditionally authorizing calls from any one of the plurality of managed code callers to the first method based upon:

a method's required level of trust; and

a level of trust attributed to the managed code caller, the level of trust attributed to the managed code caller being based upon an identification of the provider of the managed code caller and a rule demand that contains data quantifying a degree of the level of trust.

23. (Canceled)

24. (Previously Presented) The apparatus as defined in Claim 22, further comprising:

means for compiling each one of the plurality of managed code callers from an intermediate language code and metadata into native code;

means for loading the native code with a Common Language Runtime (CLR) loader in the native code portion to load the compiled native code; and

means for executing the compiled native code in the native code portion causing the managed code caller to call one method.

25. (Previously Presented) The apparatus as defined in Claim 22, further comprising means for throwing an exception when one of the plurality of managed code callers attempts to make a prevented call during the execution of the compiled native code corresponding to any one of the plurality of managed code callers.

26. (Previously Presented) The apparatus as defined in Claim 22, wherein the managed code portion further comprises one or more files associated with user code that, when compiled into an intermediate language code and metadata generated by a language compiler, are represented by one or more of the plurality of managed code callers.

27. (Previously Presented) The apparatus as defined in Claim 22, wherein the execution engine means in the native code portion further comprises a compiler to compile each one of the plurality of managed code callers into native code for execution

by the native code portion.

28. (Previously Presented) The apparatus as defined in Claim 22, wherein the execution engine means in the native code portion further comprises:

a Just In Time (JIT) compiler to compile each one of the plurality of managed code callers into native code; and

a CLR loader to load the compiled native code for execution by the native code portion.

29. (Currently Amended) A computing device, comprising:

a managed code portion including:

one or more methods in a shared managed library;

one or more assemblies placed in respective application domains for execution; and

a virtual machine;

a native code portion including:

an execution engine for the virtual machine; and

an operating system under the execution engine;

logic configured to:

intercept a call from one assembly to one method;

derive whether the call is permissible according to a prior configuration of the one of more methods, wherein:

each method provides access to a protected resource; and the prior configuration specifies whether to:

authorize the call to be made;

prevent the call to be made, the preventing being indicated by a query that determines whether a host protection custom attribute (HPCA) is associated with the one or more methods, the query determining from the HPCA that the call is to be prevented when the HPCA is associated with the one or more methods;

conditionally authorize the call to be made based upon the degree to which the one assembly is trusted by the computing device, the degree to which the computing device trusts the one assembly corresponds to an identity of a provider of the one assembly and a rule demand that contains data quantifying the degree to which the one assembly is trusted by the computing device;

provide to the one assembly access to the corresponding protected resource when the call is permissible; and

prevent access to the one assembly to the corresponding protected resource when the call is not permissible.

30. (Canceled)

31. (Canceled)

32. (Previously Presented) The computing device as defined in Claim 29, wherein the computing device compiles the one assembly into native code that is executed by a common language runtime via the operating system.

33. (Previously Presented) The computing device as defined in Claim 32, further comprising throwing an exception when:

the prior configuration specifies to attempt to make the call that is prevented; or

the prior configuration specifies to attempt to make the call when the degree to which the computing device trusts the one assembly is insufficient.

34. (Previously Presented) The computing device as defined in Claim 29, further comprising, prior to the intercepting:

determining whether the computing device will make the derivation; performing the intercepting and the deriving if the determination is affirmative; and

not performing the intercepting and the deriving if the determination is negative.

35. (Original) The computing device as defined in Claim 34, wherein:

the computing device has access to a host configuration data structure comprising:

resource checking data for making the determination; and

configuration data sufficient for the computing device's prior configuration of the one of more methods;

the determining whether the computing device will make the derivation comprises accessing, with the computing device, the resource checking data in the host configuration data structure.

36. (Previously Presented) The computing device as defined in Claim 29,

wherein the logic is further to receive intermediate language code and metadata generated by a language compiler to form the one or more assemblies for placement within respective application domains for execution.

37. (Previously Presented) The computing device as defined in Claim 36, wherein the intermediate language code and the metadata generated by the language compiler are generated from one or more files each having a file type and each being associated with user code.

38. (Previously Presented) The computing device as defined in Claim 29, wherein the execution engine further comprises:

a JIT complier to compile the assemblies into native code; and

a CLR loader to load the compiled native code for execution in the native code portion.

39. (Withdrawn) A host comprising logic for a runtime environment using a host configuration data structure containing host configuration information to disallow a call to a managed code callee from an untrusted managed code caller or to disallow a call to a managed code callee that is deemed inappropriate for the runtime environment.

40. (Withdrawn) The host as defined in Claim 39, wherein:

the host compiles the managed code caller into native code that is executed by a common language runtime via the host's operating system; and a host protection exception is thrown during the execution of the native code when the call to the managed code callee:

is made by the untrusted managed code caller; or

is deemed inappropriate for the runtime environment.

41. (Currently Amended) A host operating in a managed environment, comprising:

logic, of a computing device, for configuring each of a plurality of managed callees, each providing access to a protected resource, with a configuration that:

authorizes a call to be made to each of the plurality of managed callees for access to the corresponding protected resource;

prevents a call to be made to each of the plurality of managed callees for access to the corresponding protected resource, the preventing being indicated by a query that determines whether a host protection custom attribute (HPCA) is associated with one or more methods, the query determining from the HPCA that the call is to be prevented when the HPCA is associated with the one or more methods; or

conditionally authorizes a call to be made to each of the plurality of managed callees for access to the corresponding protected resource based upon a degree of trust of the host for one of a plurality of managed callers and a rule demand that contains data quantifying the degree of trust of the one of the plurality of managed callers, the degree of trust of the host for the one of the plurality of managed callers corresponding to an identity of a provider to the host;

logic, of the computing device, for intercepting a call from a particular one of the plurality of managed callers to a particular one of the plurality of managed callees;

logic, of the computing device, after intercepting the call, for determining whether the call is permissible according to the configuration of the particular one of the plurality of managed callees; and

logic, of the computing device, after determining whether the call is permissible, for either providing access to the particular one of the plurality of managed callers to the protected resource when the call is permissible or preventing access to the particular one of the plurality of managed callers to the protected resource when the call is not permissible.

42. (Previously Presented) The process as defined in Claim 1, wherein the managing calls comprises either authorizing or preventing a call from a first managed code caller to a first method based at least in part on the first method.